REMARKS

In an Office Action dated December 18, 2008, the Examiner has apparently withdrawn all of the previous rejections of Claims 1-4, 6-12, and 14-21 under 35 U.S.C § 103(a) as being unpatentable over various references of record, including USPN 7,142,676 issued to Hillier et al. ("Hillier") in view of USPN 6,336,121 issued to Lyson et al. ("Lyson") and USPN 6,256,733 issued to Thakkar et al. ("Thakkar"), U. S. Patent Application 2004/0151319 of Proudler ("Proudler"), and US Pub. No. 2003/0194093 issued to Evans et al. ("Evans").

Instead, the Examiner has newly rejected Claims 1, 6, 10, 15, 18, under 35 USC §102(a) as being anticipated by a passage in a textbook entitled *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, by Bruce Schneier, John Wiley and Sons (1996), Chapter 22, section 7, pages 524-525, that the Examiner refers to as the acronym NPL, presumably representing "non-patent literature," but which Applicant will refer to as "Schneier/NPL" for clarity. The Examiner has also rejected Claims 2-5, 11-14, 16, 19-21, under 35 USC §103 (a) as being unpatentable over Schneier/NPL in view of the previously cited Hillier reference.

In this response, Applicant respectfully traverses the rejections. No amendments are presented. Claims 5 and 13 have been previously canceled without prejudice. Applicant requests reconsideration of pending Claims 1-4, 6-12, and 14-21 in view of arguments as set forth in detail in the following remarks.

CLAIM REJECTIONS – 35 U.S.C. § 102

Claims 1, 6, 10, 15, 18, are rejected under 35 U.S.C. § 102 as being anticipated by Schneier/NPL. Applicant traverse the rejection. The passage on pages 524-525 reference

by the Examiner appears to describe a key distribution protocol that is apparently known as Tatebayashi-Matsuzaki-Newman (see subheading on page 524). The protocol is described as a series of numbered equations. The steps include:

(1) Alice chooses a random number r_A, and sends Trent r_A^3 mod n

(2) Trent tells Bob that someone wants to exchange a key with him.

(3) Bob chooses a random number r_B, and sends Trent r_B^3 mod n

(4) Trent uses his private key to recover r_A and r_B. He sends Alice r_A and r_B

(5) Alice calculates $(r_A + r_B) + r_A = r_B$. She uses this r_B to communicate securely with Bob.

In particular, the Examiner asserts that the equations disclose the various limitations of the independent claims as follows:

generating, by the first entity, a first key, encrypting the first key with a public key of a TPM, the TPM having at least three registers, the TPM separate from the first and second entities and having a public/private key pair, and storing the encrypted first key in a first register of the TPM as recited in Claim 1; equation (1)

generating, by the second entity, a second key, encrypting the second key with the public key of the TPM, and storing the encrypted second key in a second register of the TPM; equation (3)

decrypting, by the TPM, the encrypted first key stored in the first register and the encrypted second key stored in the second register, using the TPM's private key to obtain the first key and the second key; equation (4)

encrypting, by the TPM, the first key using the second key, and storing the first key encrypted by the second key in a third register of the TPM; equation (2)

obtaining, by the second entity from the third register of the TPM, the first key encrypted by the second key, and decrypting, by the second entity using the second key and a corresponding decryption algorithm, the first key encrypted by the second key. equation (5).

Applicant disagrees with the Examiner's conclusions. As can be seen on their face, the equations relied on by the Examiner are quite simplified. Applicant submits that they fail to disclose the limitations as recited in the claims. For example, there is nothing in equation (1) which discloses a TPM having at least three registers as recited in Claim 1. As another example, Applicant submits that Trent telling Bob that someone wants to exchange a key with him fails to disclose encrypting, by the TPM, the first key using the second key, and storing the first key encrypted by the second key in a third register of the TPM, particularly as there is no disclose that Trent is encrypting or storing anything, much less storing anything in a third register of the TPM as recited in Claim 1.

The Examiner is reminded that to anticipate a claim, the reference must disclose each and every limitation of the claim. As such, Applicant submits that, for at least this reason, the Examiner has failed to substantiate the rejection under Section 102, and respectfully requests that the Examiner withdraw the rejection of independent Claims 1, 10 and 18 under Section 102.

Dependent claims 2-4, 6-9, 11-12, 14-17 and 19-21 are allowable for at least the same reasons as independent Claims 1, 10 and 18, from which they respectively depend, as well as because of their additional limitations. Accordingly, Applicant requests the withdrawal of the rejection of dependent claims 2-4, 6-9, 11-12, 14-17 and 19-21.

CONCLUSION

For at least the foregoing reasons, Applicants submit that the rejections have been overcome. Therefore, Claims 1-4, 6-12, and 14-21 are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application. Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

April 20, 2009
Date

/Donna Jo Coningsby/
Donna Jo Coningsby
Reg. No. 41,684
Attorney for Applicant(s)

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(503) 439-8778